Market Talks
교육 센터

블록체인 · 초급 · 13강 중 11강

거래가 처리되는 과정

보내기 버튼을 누른 순간부터 코인이 도착하기까지 무슨 일이 일어나는지, 그리고 왜 때로는 예상보다 오래 걸리는지

읽는 시간 6분　　퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 11강

거래가 처리되는 과정

한 문장 요약

암호화폐 거래는 내 지갑에서 만들어지고 서명된 뒤, 노드에서 노드로 전달되고, 대기 구역에서 기다리다가 채굴자나 검증자에게 선택되며, 그 위로 새 블록이 쌓이면서 점점 깊이 묻힙니다. 내가 내는 수수료가 거래가 얼마나 빨리 대기열을 빠져나갈지를 결정합니다.

1단계: 지갑이 거래를 만들고 서명한다

보내기를 눌러도 아직 블록체인에는 아무것도 도달하지 않습니다. 먼저 지갑이 세 가지를 담은 짧은 메시지를 만듭니다. 어떤 코인을 쓰는지, 어디로 보내는지, 그리고 수수료로 얼마를 제시하는지입니다.

비트코인에서 잔액은 하나의 숫자가 아닙니다. 이전에 받은 코인 조각들이 따로따로 모여 있는 것이며, 이를 **미사용 출력**이라고 부릅니다. 0.5 BTC짜리 조각에서 0.3 BTC를 보내려면 지갑은 그 조각 전체를 사용합니다. 0.3은 받는 사람에게, 소액은 수수료로, 나머지는 **잔돈**(change)으로 내 주소로 돌아옵니다. 이더리움은 은행 잔액에 더 가깝게 작동하지만, 서명의 원리는 같습니다.

마지막으로 지갑은 8강에서 본 것처럼 내 개인 키로 메시지에 서명합니다. 서명은 소유자가 바로 이 결제를 승인했다는 것을 증명합니다. 나중에 숫자 하나만 바꿔도 서명은 더 이상 맞지 않습니다.



그림 1. 거래는 지갑에서 서명되고, 노드가 확인하고 전달하며, 멤풀에서 기다리다가 채굴자가 블록에 넣으면 첫 번째 확인을 얻습니다. 이후 블록마다 확인이 하나씩 늘어납니다.

예시: 0.5 BTC는 어디로 가는가

0.5 BTC짜리 조각 하나를 가지고 있고 친구에게 0.3 BTC를 보내려고 합니다. 지갑은 출력이 두 개인 거래를 작성합니다. 친구에게 0.3 BTC, 그리고 내 잔돈 주소로 0.1999 BTC입니다. 빠진 0.0001 BTC는 어디에도 출력으로 적히지 않습니다. 남는 금액이 곧 수수료이며, 이 거래를 블록에 넣은 채굴자가 가져갑니다.

2단계: 전파와 대기실

서명된 거래는 노드에 전달되고, 노드는 이를 확인합니다. 서명이 유효한지, 코인이 존재하는지, 이미 사용되지는 않았는지를 봅니다. 모두 통과하면 노드는 이를 피어들에게 넘기고, 7강에서 본 것처럼 몇 초 만에 네트워크 전체로 퍼집니다.

각 노드는 자신이 받은 유효한 거래를 **멤풀**(mempool, memory pool의 줄임말)이라는 대기 구역에 보관합니다. 하나의 멤풀이 있는 것이 아닙니다. 노드마다 자기 멤풀이 있어서 내용이 조금씩 다릅니다. 거래가 그곳에 있는 동안에는 **확인 0회** 상태입니다. 네트워크는 그 거래를 알고 있지만 아직 블록체인에 올라가지 않았고, 드물게는 여전히 교체될 수 있습니다.

3단계: 수수료가 순서를 정한다

비트코인 블록은 약 10분마다 생성되며 공간이 제한되어 있습니다. 대기 중인 거래가 블록 하나에 담을 수 있는 것보다 많으면, 채굴자는 차지하는 공간 대비 가장 많이 지불하는 거래부터 블록을 채웁니다. 그래서 비트코인 수수료는 금액의 비율이 아니라 **가상 바이트당 사토시**(sat/vB)라는 요율로 표시됩니다. 거래 크기가 같다면 10달러를 보내든 1,000만 달러를 보내든 비용은 같습니다.

네트워크 상황	보통 일어나는 일
한산한 멤풀	낮은 수수료로도 다음 블록이나 그다음 블록에 들어감
붐비는 멤풀	낮은 수수료 거래는 기다려야 하며, 때로는 몇 시간 또는 며칠
갑작스러운 몰림	한 시간 안에 수수료가 몇 배로 뛸 수 있음

몰림은 극단적일 수 있습니다. 2024년 4월 20일, 비트코인 채굴 보상을 절반으로 줄인 블록인 840,000번 블록은 37 BTC가 넘는 수수료를 거뒀는데, 당시 가치로 약 240만 달러였습니다. 많은 사용자가 그 역사적인 블록에 들어가려고 경쟁했기 때문입니다.

비유: 저녁의 마지막 여객선

작은 여객선이 10분마다 정해진 좌석 수로 출발합니다. 조용한 밤에는 모두가 탑니다. 연휴 주말에는 줄이 길어지고, 승무원은 좌석당 가장 높은 요금을 제시한 사람부터 태웁니다. 최저 요금을 제시했다면 다음 배가 와도, 그다음 배가 와도 여전히 줄에 서 있게 됩니다.

4단계: 확인과 결제 완료

채굴자가 내 거래를 네트워크가 받아들이는 블록에 넣으면 거래는 **확인 1회**를 얻습니다. 그 위에 블록이 하나 쌓일 때마다 확인이 하나씩 늘어납니다. 블록이 추가될수록 결제를 되돌리기는 더 어려워지는데, 6강에서 설명했듯이 공격자가 그 블록들을 모두 다시 만들어야 하기 때문입니다.

확인 횟수(비트코인)	일반적인 의미
0	네트워크가 보았지만 아직 블록에 없음
1	블록에 포함됨, 일상적인 소액에는 충분
여러 번	거래소가 입금을 반영하기 전에 보통 기다리는 횟수로, 플랫폼마다 다름
6	큰 금액에 대한 오래된 경험칙, 약 1시간

다른 네트워크는 각자의 리듬이 있습니다. 이더리움은 12초마다 블록을 추가하고, 약 13분 후에 블록을 최종 확정된 것으로 봅니다. 그 시점부터는 엄청난 양의 스테이킹된 ETH를 소각하지 않고는 되돌릴 수 없습니다.

거래가 멈춰 있을 때

붐비는 시기에 수수료를 너무 낮게 설정하면 거래가 멤풀에서 오랫동안 기다릴 수 있습니다. 잃는 것은 없습니다. 코인은 아직 떠나지 않았습니다. 아주 오래된 거래는 결국 대부분의 멤풀에서 삭제되고, 코인은 원래 있던 곳에 그대로 남습니다. 흔히 쓰는 해결책은 두 가지입니다.

- **수수료 대체(Replace-by-fee, RBF).** 지갑이 같은 결제를 더 높은 수수료로 새로 보내 기존 거래를 대체합니다.
- **자식이 부모 비용 지불(Child pays for parent, CPFP).** 받는 사람이, 또는 내가 잔돈을 통해 멈춘 코인을 높은 수수료의 새 거래에서 사용하면, 채굴자에게 두 거래를 함께 넣을 이유가 생깁니다.

어떤 방법을 쓰든 전체 과정을 직접 추적할 수 있습니다. 모든 거래에는 **txid**라는 ID가 있으며, 이를 블록 탐색기에 붙여 넣으면 대기 중인지, 확인되었는지, 얼마나 깊이 묻혔는지 볼 수 있습니다.

트레이더에게 왜 중요한가

- **입금은 즉시 이루어지지 않습니다.** 거래소는 요구하는 확인 횟수를 채운 뒤에야 비트코인을 반영합니다. 빠른 움직임에 맞춰 거래할 계획이라면 코인은 움직임이 오기 전에 이미 거래소에 있어야 하며, 이동 중이어서는 안 됩니다.
- **시장이 움직이면 수수료가 오릅니다.** 급격한 가격 변동은 많은 사람을 동시에 블록체인으로 불러들이고, 수수료도 함께 뜁니다. 보내기 전에 현재 수수료율을 확인하고, 타이밍이 중요할 때는 가장 낮은 설정을 고르지 마세요.
- **txid를 보관하세요.** 입금이나 출금이 늦어지는 것 같으면 txid로 정확한 위치를 알 수 있습니다. 거래소 고객 지원이 가장 먼저 요청하는 정보이기도 합니다.

핵심 용어

멤풀	각 노드가 블록에 포함되기를 기다리는 유효한 거래를 보관하는 대기 구역.
거래 수수료	거래를 블록에 포함시키기 위해 보내는 사람이 내는 비용. 비트코인에서는 입력에서 출력을 빼고 남는 금액입니다.
sat/vB	가상 바이트당 사토시. 비트코인 수수료를 비교할 때 쓰는 요율입니다. 1사토시는 1억분의 1 비트코인입니다.
확인	체인에서 내 거래를 담고 있거나 그 뒤에 이어진 블록 하나. 확인이 많을수록 결제를 되돌리기 어렵습니다.
잔돈 출력	사용된 코인 중 지갑이 보내는 사람 자신의 주소로 돌려보내는 부분.
거래 ID(txid)	거래를 식별하는 고유 코드로, 블록 탐색기에서 거래를 조회할 수 있게 해 줍니다.

핵심 정리

1. 거래는 네트워크로 무언가를 보내기 전에 내 지갑에서 만들어지고 서명됩니다.
2. 노드는 거래를 확인하고 전달하며 각자의 멤풀에 보관하는데, 이때 확인은 0회입니다.
3. 블록 공간은 제한되어 있으므로 채굴자는 금액이 가장 큰 거래가 아니라 수수료율이 가장 높은 거래를 고릅니다.
4. 내 블록 뒤에 블록이 하나 추가될 때마다 확인이 하나씩 늘고, 거래소는 정해진 횟수를 기다린 뒤 입금을 반영합니다.

5. 멈춘 거래는 수수료 대체나 자식이 부모 비용 지불 방식으로 앞당길 수 있고, txid로 추적할 수 있습니다.

실력 점검

각 문제에 답을 하나씩 표시하세요. 해설이 포함된 정답은 다음 페이지에 있습니다. markettalks.info에서 온라인으로 퀴즈를 풀고 바로 점수를 확인할 수도 있습니다.

1. 거래는 어디에서 서명되나요?

- A 거래를 처음 받은 노드에서
- B 보내기 전, 보내는 사람의 지갑에서
- C 거래를 블록에 넣는 채굴자가
- D 도착했을 때 받는 사람의 지갑에서

2. 0.3 BTC를 보내려고 0.5 BTC짜리 코인을 사용합니다. 나머지는 어떻게 되나요?

- A 영원히 사라진다
- B 다음 반감기까지 잠겨 있다
- C 대부분은 잔돈으로 나에게 돌아오고, 남는 소액이 수수료가 된다
- D 받는 사람이 팁으로 가진다

3. 멤풀이란 무엇인가요?

- A 블록을 기다리는 유효한 거래를 각 노드가 보관하는 대기 구역
- B 비트코인 개발자들이 운영하는 단일 글로벌 서버
- C 거래소의 코인을 보관하는 지갑
- D 블록에서 수수료가 기록되는 부분

4. 크기가 같은 비트코인 거래 두 건이 있습니다. 하나는 10달러, 다른 하나는 1,000만 달러를 보냅니다. 빨리 포함되려면 어느 쪽이 더 높은 수수료가 필요할까요?

- A 1,000만 달러 거래, 수수료가 비율로 매겨지기 때문에
- B 어느 쪽도 아니다, 같은 수수료율이 필요하다
- C 10달러 거래, 소액 결제는 지연되기 때문에
- D 수수료는 네트워크가 아니라 거래소가 정한다

5. 내 거래가 블록에 들어갔고, 그 뒤로 블록 두 개가 더 추가되었습니다. 확인은 몇 회인가요?

A 1회
B 2회
C 3회
D 6회

6. 붐비는 시기에 낮은 수수료로 보낸 거래가 몇 시간째 기다리고 있습니다. 표준적인 해결책은 무엇인가요?

A 같은 코인을 새 주소로 다시 보낸다
B 채굴자에게 연락해 포함시켜 달라고 요청한다
C 시드 문구로 지갑을 복구한다
D 수수료 대체로 더 높은 수수료의 새 버전을 보낸다

정답 및 해설

1 B

보내기 전, 보내는 사람의 지갑에서

지갑은 전파하기 전에 개인 키로 서명합니다. 노드와 채굴자는 서명을 확인할 뿐 만들 수는 없습니다.

2 C

대부분은 잔돈으로 나에게 돌아오고, 남는 소액이 수수료가 된다

비트코인은 코인을 통째로 사용합니다. 지갑은 차액을 내 잔돈 주소로 보내고, 약간을 할당하지 않고 남겨 수수료로 삼습니다.

3 A

블록을 기다리는 유효한 거래를 각 노드가 보관하는 대기 구역

노드마다 자기 멤풀이 있으므로 단 하나의 멤풀은 없습니다. 멤풀에는 유효하지만 아직 블록에 들어가지 않은 거래가 있습니다.

4 B

어느 쪽도 아니다, 같은 수수료율이 필요하다

채굴자는 공간의 가상 바이트당 수수료를 비교합니다. 보내는 금액은 상관없고 거래의 크기만 중요합니다.

5 C

3회

거래를 담은 블록이 첫 번째 확인이고, 그 뒤의 블록마다 하나씩 더해지므로 1 더하기 2는 3입니다.

6 D

수수료 대체로 더 높은 수수료의 새 버전을 보낸다

수수료 대체는 대기 중인 거래를 더 높은 수수료의 버전으로 바꿉니다. 다른 흔한 방법은 자식이 부모 비용 지불입니다.

출처

- Bitcoin Developer Guide, 거래: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph, 비트코인 사용자들이 반감기 블록에 사상 최대인 240만 달러의 수수료를 지불: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org, 지분 증명과 최종성: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech, Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

계속 학습하기

다음: 12강
퍼블릭, 프라이빗, 컨소시엄 블록체인

이 강의는 MARKET TALKS 교육 센터의 무료 블록체인 과정에 속합니다. 초급, 중급, 고급 강의로 구성되며 강의마다 퀴즈와 다운로드 가능한 PDF가 제공됩니다.

교육 센터
기초 원리부터 고급 주제까지 다루는 강의

시장 분석
주요 시장에 대한 기술적 분석과 기본적 분석

리포트
비트코인, 금, 은, SPX 등

markettalks.info

텔레그램 @MARKET_TALKS

교육 목적으로만 제공됩니다. 이 문서의 어떤 내용도 투자 조언이 아닙니다. © 2026 MARKET TALKS. 이 PDF는 수정 없이 자유롭게 공유하실 수 있습니다.